8

Question 1:

Answer the following questions by clearly circling *the most appropriate* answer (1 point *each*)

1. A loss of _____ is the unauthorized disclosure of information.
   a. integrity
   b. authenticity
   c. reliability
   d. confidentiality

2. The OSI security architecture focuses on the following aspects of information security:
   a. protocols, key management and attacks
   b. attacks, mechanisms and services
   c. protocols, attacks and defenses
   d. attacks, defenses and firewalls
   e. key production, key exchange and key management

3. What type of crypto-analytical attack where an adversary has least amount of information to work with?
   a. Known plain text
   b. Cipher text only
   c. Plain text only
   d. Chosen cipher text

4. The practice of embedding a message in a document, image, video or sound recording so that its very existence is hidden is called
   a. anonymity.
   b. steganography.
   c. non-repudiation.
   d. masquerading

5. When an attacker performs a capture of a data unit and its subsequent retransmission to produce an unauthorized effect, which attack he is performing?
   a. Disruption
   b. Replay
   c. Masquerade
   d. Service denial
   e. Unauthorized change of the content

6. An encryption scheme that requires large quantities of random keys that are as long as the messages that have to be encrypted, and are distributed on a regular basis to both sender and receiver, is known as:

   a. Key-pad scheme
   b. iPad scheme
   c. crypto-pad scheme
   d. time-pad scheme
   e. one-time pad scheme

7. What characteristic of Digital Encryption Standard (DES) used in Electronic Code Book (ECB) mode makes it unsuitable for long messages?

   a. Block fragmentation causes message cipher instability.
   b. Weak keys will produce symmetrical message holes.
   c. Each message block produces a single cipher text block.
   d. Repeated message blocks produce repeated cipher text blocks.

8. In AES, the first and the last round begin with the following reversible part:

   a. MixColumns
   b. AddRoundKey
   c. ShiftRows
   d. Substitute bytes
   e. KeyExpand

9. How many S-boxes does AES have?

   a. 5
   b. 1
   c. 3
   d. 16
   e. 8

10. A way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is:

    a. polyalphabetic substitution cipher
    b. vernam cipher
    c. product cipher
    d. rail fence cipher

6.5

Question 2:

1. Define each of the following: [2 points]

   - Cryptanalysis

~~The knowledge of the criteria methods.~~

Analysing the methods and the enhance in the ~~of cryptology~~ cryptography.

   - unconditional security

No matter how much power and speed do the have, the cipher can't be broken

2. We can encrypt and decrypt messages written with the full German alphabet. The German alphabet consists of the English letters together with the three umlauts, Ä , Ö , Ü , and the (even stranger) "double s" character ß. [2 points]

   a. How large is the key space using monoalphabet?

   30 X 30 = 900

   b. Monoalphabetic substitution cipher is not secure. Why?

Because of the language characteristic, where there are letter are commonly used more than others.

3. Playfair and polyalphabet algorithms both use a keyword. However, polyalphabet is considered better than playfair. Why? [2 points]

Because Playfair is still have some language characteristic, where each two letters will be replaced by the same two letters, but in polyalphabet there is big chance of changing the cipher letter.

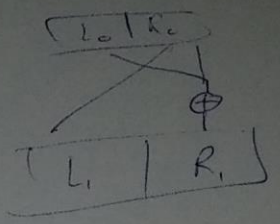
4. Explain what is brute force attack and why it's not the preferred method of attack [2 points]

It's cheking all possible keys one by one.
It's not prefered because keys are usually very big, so it's difficult to go through all of the possible keys.

5. Explain why in one-time pad algorithm repeating the key is not secure. [2 points]

Because it gives the attacker more information about what might be the key.

10



Question 3:

1. How many rounds have DES, how big is the key and how big is the block? [1 points]

1 16 round, 56 bit, 64 bit

2. Given the following symbols used in DES { L_0, R_0, F, XOR, L_1, R_1, K_1 } [4 points]

i. Write the encryption equations to produce L_1 and R_1 for one round of DES from L_0 and R_0

2 $L_1 = R_0$

$R_1 = L_0 \oplus f(R_0, key)$

ii. Write the decryption equations to produce L_0 and R_0 from L_1 and R_1 calculated in (a) and prove the equality.

$R_0 = L_1$

2 $L_0 = R_1 \oplus f(R_0, key)$

$L_0 = L_0 \oplus F(R_0, key) \oplus F(R_0, key)$

$L_0 = L_0 \oplus 0$

$L_0 = L_0$

3. Explain the Feistel Cipher Structure? [2 points]

2 The plaintext will be partitioned into two halves, and in every stage there will be swapping and then XORing the left part with key.

4. Construct a table for the Playfair Cipher with the keyword INTRAVASCULAR? [3 points]

Then encrypt the phrase: "CREATIVE"

I/J	N	T	R	A
V	S	C	U	L
B	D	E	F	G
H	K	M	O	P
Q	W	X	Y	Z

CREATIVE

⇒ UTGTRNCB

3

⇒ UTGTRNCB

5/2

Question 4:

1. List two advantages of Counter Block mode. [1 points]
   i. Same block can have different ciphertext.
   ii. Avalanche effect ×

2. What is the rationale of the following stages of AES [2 points]
   i. Shift Row Difusion
   ii. Byte Substituion confusion

3. An algorithm designer modified AES Encryption algorithm by swapping the byte substitution and shift row stages. i.e. first perform shift row then byte substitution and claimed that his algorithm is better. Is it? Why? [1 points]
   NO, because the same result will appear weather you shifted the raws first or you subsituted the values.

4. Explain 2DES meet in the middle attack. [2 points]
   2DES will Encrypt the massage twice using the DES and two different keys

5. DES and AES both exhibit strong avalanche effect, however, AES is better. Explain how AES is better. [4 points]
   - In AES, the avalanche effect will appeare clearly after two stages, where most of the bytes will be changed, unlike the DES where it will happen in the late stages.
   - AES use bigger key size than DES which make it much harder to break.

ANSWER IS Back (:)

- In AES, the avalanche happen because there is a mixing stages so any change in any bit, this will affect the Result. 1½

- In DES, the effect happen because any change will effect the matrix. ??